REMARKS

No claim has been amended. Claims 2-14 and 16-21 remain in the application.

Claim Rejections – 35 U.S.C. §103(a)

Claims 2-14 and 16-21 stand finally rejected under 35 U.S.C. §103(a) as allegedly being unpatentable as obvious over Rowland (US 6,405,318) in view of Baker (US 6,775,657). This rejection is again traversed.

The claimed invention relates to a system and corresponding method for detecting the state of a computer network. As set forth in amended claim 2, the system includes:

> agents disposed in said computer network, each said agent comprising:
>
> data collection means for passively collecting, monitoring, and aggregating data representative of activities of respective nodes within said computer network;
>
> means responsive to the data from the data collection means for analyzing said data to develop activity models representative of activities of said network in a normal state and activities of said network in an abnormal state; and
>
> means for comparing collected data to said activity models to determine the state of said computer network at different times and to dynamically update said activity models,
>
> wherein said analyzing means performs a pattern analysis on the collected data and said comparing means compares the results of the pattern analysis of data collected by an agent to the results of pattern analysis of data collected by analyzing means of other agents to identify similar patterns of suspicious activity in different portions of the computer network.

Claim 18 recites a corresponding method of detecting the state of a computer network. Such a system and method is not taught or suggested by Rowland and Baker taken separately or together.

In the Final Rejection, the examiner maintained the previous rejections over Rowland and Baker. In the "Response to Arguments" section at page 2 of the Final Rejection, the examiner rebutted Applicant's previous arguments by making several observations underlying the examiner's obviousness determination. Applicant believes these observations

to be erroneous and that, accordingly, the examiner has failed to establish *prima facie* obviousness. Applicant will address the examiner's observations in turn.

First, the examiner alleges that Applicant's arguments fail to comply with 37 CFR 1.111(b) as allegedly amounting to "general allegations that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references" and do not comply with 37 CFR 1.111(c) as allegedly failing to point out the patentable novelty that the claims present in view of the disclosures of the references or the objections made. The examiner further alleges that the Applicant does not show how the amendments avoid such references or objections. Applicant strongly disagrees.

Contrary to the examiner's allegations, Applicant noted at page 7, lines 20-23, of the November 3, 2008 Response the examiner's acknowledgment that Rowland does not teach the recited feature of comparing "the results of the pattern analysis of data collected by an agent to the results of pattern analysis of data collected by analyzing means of other agents to identify similar patterns of suspicious activity in different portions of the computer network" as recited in the language at the end of independent claims 1 and 18. Applicant then specifically noted at page 8, lines 3-13, of the November 3, 2008 Response that Baker does not teach such features either. Applicant then notes at page 8, lines 14-19, of the November 3, 2008 Response that since neither Rowland nor Baker teach this claimed feature that the combination would not suggest how to identify patterns of suspicious activities at different portions of the computer network as so claimed. Applicant submits that its argument is quite straightforward and clearly in compliance with 37 CFR 1.111(b) and (c).

Second, the examiner disagrees with Applicant's assertion that "Baker nowhere suggests that pattern analysis is conducted by multiple agents in a network so that patterns of suspicious activities at different ports of the computer network may be determined." In rebuttal, the examiner refers to Figures 2 and 3 of Baker and the associated text at column 5, lines 10-14 and 29-45 and concludes that such teachings as combined with Rowland would have rendered obvious to one skilled in the art the recited feature of comparing "the results of the pattern analysis of data collected by an agent to the results of pattern analysis of data collected by analyzing means of other agents to identify similar patterns of suspicious activity in different portions of the computer network."

Again, Applicant submits that Baker does not teach that pattern analysis is conducted by multiple agents in a network as claimed. As previously noted, Baker teaches a method of monitoring activity on a network and maintaining a registry of each host node address of a host node that is capable of performing host-based intrusion detection services. During operation, the destination address of the monitored network activity is checked against the registry to determine if the destination address is that of a registered node that is capable of performing host-based intrusion detection services. If the destination address matches that of a registered node, the network activity is allowed to proceed unencumbered to the registered destination node. On the other hand, if the destination address is not in the registry, then intrusion detection services are performed "either by host-based intrusion detection services available on the network node 120 or by network-based intrusion detection services available on network node 120. Additionally, the data transmission may be passed by network node 120, to another node, host or network, having the ability to perform intrusion detection services on the data transmission." (Figure 1; see column 5, lines 29-37). Thus, Baker teaches that the intrusion detection services are performed at the destination node, on the network node 120, or passed to another node, host or network to be performed. Nowhere does Baker suggest that multiple nodes perform an intrusion detection service and compare results. Baker thus does not teach or suggest that such intrusion detection services may be performed by "multiple agents in a network so that patterns of suspicious activities at different ports of the computer network may be determined" as claimed. On the contrary, it is quite clear that Baker teaches that the intrusion detection services for a message are performed by the destination node if it is in the registry, or by a designated node if the destination node is not in the registry. A single node performing intrusion detection services for a message cannot be understood by one skilled in the art to be equivalent to plural "agents" that compare "the results of the pattern analysis of data collected by an agent to the results of pattern analysis of data collected by analyzing means of *other agents* to identify *similar patterns of suspicious activity in different portions of the computer network*" as claimed. Such comparisons are not taught by Baker.

Third, and finally, the examiner alleges that Applicant cannot rely upon the feature of "multiple agents" as that feature is allegedly not recited in the rejected claims. Again, Applicant disagrees. Independent claim 1 plainly recites a system that detects the state of a

computer network, comprising "***agents*** disposed in said computer network, ***each said agent comprising***...." "Agents" is clearly recited in the plural. Similarly, independent claim 18 includes the step of "providing ***agents*** disposed in said computer network to passively collect, monitor, and aggregate data representative of activities of respective nodes within said computer network." Again, "agents" is clearly recited in the plural. The examiner's allegations that multiple agents are not recited in the claims is clearly erroneous.

Now, turning back to the rejections, Applicant again submits that Rowland discloses an intrusion detection system that monitors a computer system in real-time to identify activity indicative of attempted or actual access by unauthorized persons or computers. In the embodiment of Figure 9, the system includes a central controller in a network that contains multiple host computers 151-153. Each host computer 151-153 includes the monitoring software and sends information about log auditing, login anomaly detection, etc. to the central controller for centralized auditing of events 154, data analysis 155, cross-correlation of intrusion activity throughout the network 156, and alerting the network system administrator 157 if anomalous activity is found. Rowland thus teaches the use of a central controller for performing the intrusion detection activities.

As noted above, Baker teaches that the intrusion detection services are performed on a destination node if it is in the registry and, if not in the registry, by a network node 120 or another node, host or network.

Accordingly, neither Rowland nor Baker teaches a system that detects the state of a computer network, where the system comprises not one, but plural "***agents***" disposed in a computer network, where "***each said agent***" includes "comparing means [that] compares the results of the pattern analysis of data collected by ***an agent*** to the results of pattern analysis of data collected by analyzing means of ***other agents*** to identify similar patterns of suspicious activity in ***different portions of the computer network***" as claimed in independent claims 1 and 18. No such plural agents and no such comparison are taught by Rowland and/or Baker. The examiner's conclusions to the contrary are not supported by the teachings of Rowland and Baker.

For at least these reasons, the rejection of claims 2-14 and 16-21 as being unpatentable as obvious over Rowland in view of Baker is improper and withdrawal of this rejection is respectfully solicited.

Conclusion

For the reasons set forth herein, claims 2-14 and 16-21 are believed to be in condition for allowance. A Notice of Allowability is solicited.

Date: June 5, 2009

/Michael P. Dunnam/
Michael P. Dunnam
Registration No. 32,611

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439